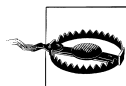


KAPITEL 14

Juristische Aspekte beim Einsatz von Spam- und Virenfiltern

Neben allen technischen Problemen wirft das Filtern von E-Mail auch rechtliche Probleme auf. Den meisten Administratoren ist gar nicht bewusst, dass sie sich auf juristisch gefährlichem Terrain bewegen, wenn sie E-Mails auf Spam filtern. Obwohl das Versenden von Spam-E-Mails nach einem Urteil des Bundesgerichtshofs (BGH) vom 11.03.2004 (I ZR 81/01) sittenwidrig ist, bringt das Prüfen und Filtern von E-Mails eine Reihe von gesetzlichen Problemen mit sich. Die meisten davon lassen sich durch entsprechende Kenntnis und vorbereitende Maßnahmen allerdings zumindest minimieren. In diesem Kapitel wird versucht, auf die dabei entstehenden rechtlichen Probleme hinzuweisen und Anleitungen zur Vermeidung von rechtlichen Stolperfallen zu geben.



Dieses Buch kann, darf und will keine rechtliche Beratung geben. Im Zweifelsfall sollte man einen ausgebildeten Juristen befragen. Dabei ist anzumerken, dass sich die deutsche Rechtsprechung in einigen Aspekten der rechtlichen Folgen von Spam-Filterung uneinig ist, also die bereits existierenden Urteile keine Garantie geben, dass ein anderes Gericht in einem ähnlichen Fall genauso urteilen würde.

Rechtliche Handhabe gegen Spam

Das Versenden von Spam ist in Deutschland seit Ende Oktober 2003 durch die Umsetzung der europäischen Datenschutzrichtlinie in deutsches Recht reguliert worden. Durch die Novellierung des Gesetzes gegen den unlauteren Wettbewerb (UWG) wurden Spam-E-Mails explizit als Beispiel für unlautere Werbung aufgenommen. So heißt es in § 7 UWG:

Unlauter im Sinne von § 3 handelt insbesondere, wer (...) einen Marktteilnehmer in unzumutbarer Weise belästigt, insbesondere durch (...) die Verwendung von automatischen Anrufmaschinen, Faxgeräten oder elektronischer Post für Zwecke der Werbung, ohne dass ein ausdrückliches oder stillschweigendes Einverständnis der Adressaten vorliegt.

Das Fälschen oder Verschleiern von Absenderadressen gilt ebenfalls als unzumutbare Belästigung nach § 7 Abs. 2 Nr. 4 des UWG:

4. bei einer Werbung mit Nachrichten, bei der die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird oder bei der keine gültige Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

Zusätzlich liegt nach Meinung der meisten Juristen bei Spam an Privatpersonen eine Verletzung des Persönlichkeitsrechts vor.

Aus diesen Umständen ergibt sich ein Unterlassungsanspruch nach § 823 Abs. 1 in Verbindung mit § 1004 BGB.

In der Praxis bedeutet die klare rechtliche Lage allerdings wenig. Spam-Versender Nr. 1 sind immer noch die USA, dicht gefolgt von Korea und China. Der Versuch, deutsches Recht in den USA oder gar in Fernost durchzusetzen, wird vermutlich von sehr hohen Kosten und einer geringen Chance auf Erfolg begleitet sein.

Weil ein Großteil des Spams durch Backdoors oder offene Relays verschickt wird, bekommt man die wahren Urheber von Spam leider selten zu fassen. Daher wird man in den meisten Fällen daran gebunden sein, Spam anderweitig loszuwerden.

Wenn man jedoch gegen einen Spammer vorgehen möchte, sollte man einen auf Online-Recht spezialisierten Anwalt beauftragen, damit dieser den Spammer abmahnt. Es ist auch möglich, selbst eine Abmahnung zu schreiben. Wegen der damit verbundenen rechtlichen Risiken sollte man sich dies jedoch gut überlegen und nicht voreilig handeln. Sollte man sich entscheiden, eigenhändig gegen Spammer vorzugehen, findet man unter <http://www.recht-im-internet.de> entsprechende Musterbriefe.

Rechtliche Handhabe gegen Viren

Die rechtliche Lage bei Viren ist ziemlich eindeutig. Das Verbreiten von Viren ist in der Regel nach § 303a StGB strafbar:

(1) Wer rechtswidrig Daten (...) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Wenn durch Viren oder Würmer die Computer einer Firma oder einer Behörde geschädigt werden, kommt zusätzlich noch der Straftatbestand der Computersabotage zum Tragen (§ 303b StGB):

(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, daß er

1. eine Tat nach § 303a Abs. 1 begeht oder

2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Dies gilt aber nur bei einer fahrlässigen oder wissentlichen Verbreitung von Schadprogrammen. Die unabsichtliche Verbreitung von Viren ist – aus nachvollziehbaren Gründen – nicht strafbar.

Rechtliche Folgen bei der Analyse von E-Mails

Die elektronische Analyse von E-Mails wirft in erster Linie datenschutzrechtliche Probleme auf. Der E-Mail-Verkehr unterliegt hierbei den Bestimmungen des Telekommunikationsgesetzes (TKG) und des Bundesdatenschutzgesetzes (BDSG).

In § 4 Abs. 1 des Bundesdatenschutzgesetzes heißt es:

(1) Die Verarbeitung personenbezogener Daten und deren Nutzung sind nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.

Das bedeutet in der Praxis, dass jede Erhebung von Daten ohne Einwilligung des Betroffenen nicht gestattet ist. Das elektronische Analysieren einer E-Mail auf Spam-Verdacht fällt bereits unter die Erhebung von Daten.

Bei der Analyse gibt es allerdings auch Ausnahmen. So ist das Prüfen einer E-Mail auf Virenverdacht aus Gründen des Systemschutzes durchaus zulässig (§ 28 Abs. 1 Nr. 2 BDSG):

(1) Das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

(...)

2. soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung überwiegt

Die dabei erfassten Daten, also die E-Mail, dürfen allerdings nicht anderweitig verwendet werden (§ 31 BDSG), also auch nicht zur Spam-Prüfung.

Auch hierbei gibt es wiederum Ausnahmen. Im Fall einer Betriebsstörung durch Spam-Wellen oder Überlastung der Systeme gilt das Identifizieren und Löschen dieses Spams im Rahmen des Systemschutzes durchaus als gerechtfertigt.

Als Betreiber von E-Mail-Diensten unterliegt man des Weiteren dem Fernmeldegeheimnis. Hierbei ist es unwichtig, ob dabei Gewinnerzielungsabsicht zu Grunde liegt (§ 3 Nr. 5 TKG). So sind beispielsweise auch Administratoren in Hochschulen dem Fernmeldegeheimnis unterworfen. Dazu § 85 Abs. 2 des TKG:

(2) Zur Wahrung des Fernmeldegeheimnisses ist verpflichtet, wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

In juristischer Hinsicht strittig ist, ob eine Firma, in der ausschließlich dienstlicher E-Mail-Verkehr gestattet ist, auch dem Fernmeldegeheimnis unterliegt. Es gibt zu dieser Sachlage noch kein obergerichtliches Urteil. Bis ein solches gesprochen wird, sollte man davon ausgehen, dass Mitarbeiter, die ihren Internetzugang lediglich dienstlich nutzen, auch durch das Fernmeldegeheimnis geschützt sind.

Zusammenfassend lässt sich festhalten, dass ohne die Einwilligung der Nutzer lediglich das Prüfen der E-Mails im Rahmen des Systemschutzes gestattet ist. Für alles, was darüber hinausgeht, sollte die Einwilligung der Nutzer eingeholt werden.

Rechtliche Folgen bei der Filterung von E-Mails

Das Oberlandesgericht Karlsruhe hat am 10.01.2005 entschieden, dass Administratoren, die E-Mails filtern oder blocken, sich damit unter Umständen strafbar machen. Dies ist eine Folge daraus, dass E-Mails unter den Begriff der Telekommunikation fallen. Laut § 3 Nr. 16 TKG ist Telekommunikation »der technische Vorgang des Aussendens, Übermittels und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen«. Darunter fallen auch E-Mails.

Das bedeutet, dass sich ein Administrator, der E-Mails filtert oder blockiert, nach § 206 Abs. 2 StGB (Verletzung des Post- oder Fernmeldegeheimnisses) strafbar machen kann. Insbesondere könnte der Einsatz von Filtern eine Unterdrückung der Sendung darstellen, was nach § 206 Abs. 2 Nr. 2 StGB strafbar ist. Unterdrückt im Sinne des § 206 ist eine E-Mail dann, wenn sie dem normalen Telekommunikationsverkehr entzogen wird. Hierbei reicht bereits ein »Zurückhalten«, was beim Einsatz einer Quarantäne schon der Fall ist. Dadurch gilt jede E-Mail, die in einem dem Nutzer nicht zugänglichen Ordner gespeichert wird, als unterdrückt. Strafbar ist der ganze Vorgang jedoch nur dann, wenn er unbefugt durchgeführt wird. Dem Problem kann also durch das Einholen einer Erlaubnis des Nutzers beigegeben werden.

Interessanterweise ist auch jede Veränderung einer E-Mail strafbar (§ 303a StGB – Datenveränderung). Verboten ist dabei wie oben zitiert das rechtswidrige Löschen, Unterdrücken und Verändern von Daten. Bereits das Markieren einer Spam-E-Mail im Header gilt hierbei als strafrechtlich relevante Datenveränderung. Aber auch hier gilt das nur für unbefugtes Verändern der E-Mail – und nicht, wenn eine Erlaubnis des Nutzers vorliegt. Das Vorgehen gegen Viren und andere Schädlinge ist wiederum durch Notwehr beziehungsweise zur Vermeidung von Betriebsstörungen abgesichert.

Es ist zu beachten, dass die Strafandrohungen stets die Person betreffen, die die Tat durchgeführt hat, unabhängig davon, ob sie dazu etwa im Rahmen ihrer beruflichen Tätigkeit angewiesen worden war. Aber auch andere Beteiligte sind nicht vor Rechtsfolgen sicher. § 206 StGB (Verletzung des Post- oder Fernmeldegeheimnisses) sieht unter anderem vor, dass auch jemand bestraft wird, der die bezeichneten Handlungen gestattet oder fördert. Darüber hinaus könnten Beteiligte möglicherweise wegen Beihilfe oder Anstiftung belangt werden.

Problembewältigung

Um die rechtlichen Risiken für den Systemadministrator und das Unternehmen abfangen zu können, bieten sich zwei sinnvolle Möglichkeiten zur Auswahl an.

Nutzungsbedingungen

Die Benutzung des E-Mail-Diensts wird von einer Richtlinie abhängig gemacht, der der Benutzer zustimmen muss. In dieser sollte enthalten sein, dass Spam-Filter-Software eingesetzt wird und E-Mails unter Umständen einer Filterung unterliegen. Der Vollständigkeit halber sollten auch einige technische Details erwähnt werden, zum Beispiel wenn man externe DNS-Blackhole-Lists verwendet und so bestimmte Hosts oder Netze vom E-Mail-Verkehr ausschließt.

Aktivierung durch den Nutzer

Wenn der Benutzer den Spam-Filter selbst einschalten muss, zum Beispiel durch ein Web-Interface, gibt er damit seine Zustimmung für den Einsatz des Spam-Filters.

In Unternehmen sollte man in Zusammenarbeit mit dem Betriebsrat oder der Personalvertretung versuchen, eine Betriebsvereinbarung zum Thema Filterung von E-Mails zu erarbeiten. Auf jeden Fall sollte vermieden werden, dass sich Mitarbeiter übergangen oder sogar überwacht fühlen. Sonst können dem Unternehmen und den verantwortlichen Personen schnell rechtliche Probleme ins Haus stehen. Systemadministratoren müssen sich bewusst sein, dass sie sich ohne derartige Absicherungen möglicherweise strafbar machen, selbst wenn sie zu den Handlungen von Vorgesetzten angewiesen worden sind.

